Das war kein wirklicher Angriff, aber es hätte sein können.

Dies war ein simulierter Angriff, um Mitarbeiter über die Gefahren von Phishing und Social Engineering aufzuklären.

Solche oder ähnliche E-Mails werden aber tatsächlich von Hackern verschickt um Mitarbeiter zum „Klicken“ zu verführen.

Deswegen bitte immer Vorsicht mit Links und Anhängen! Stellen Sie immer folgende Fragen:

- **Kenne ich den Absender? Erwarte ich eine E-Mail wie diese?**
- **Stimmt der angegebene Absendername mit der tatsächlichen Absender Adresse überein?**
- **Gibt es Unstimmigkeiten im Text oder Betreff?**
- **Werde ich unter Druck gesetzt zu klicken? (nur noch heute, bald wird das Konto gesperrt, usw…)**

Falls Sie bei einer E-Mail Zweifel haben, bitte zuerst auf anderem Wege (z.B. Telefon) vergewissern, dass die E-Mail legitim ist, bevor Sie einen Link klicken oder eine Datei öffnen. Sie können verdächtige E-Mails auch an Ihren Datenschutzbeauftragten oder die IT melden, löschen, oder einfach nicht darauf reagieren.